SECS 1030

labo 5 – Malware – analyse dynamique

Noté sur 18 points, 10% de la note finale à rendre pour jeudi 21 novembre

Objectif du laboratoire : Analyser une application potentiellement malveillante par analyse dynamique dans une SandBox

Machine virtuelle : **Windows SandBox** sans réseau sur le VPN CCNB.

Configuration Windows Sandbox 2 points, puis 2 points par question pour les 4 exercices (soit 16 points).

Important : Les fichiers 0.exe, 1.exe, 2.exe, 3.exe doivent être exécutés uniquement dans la Windows Sandbox (bac à sable).

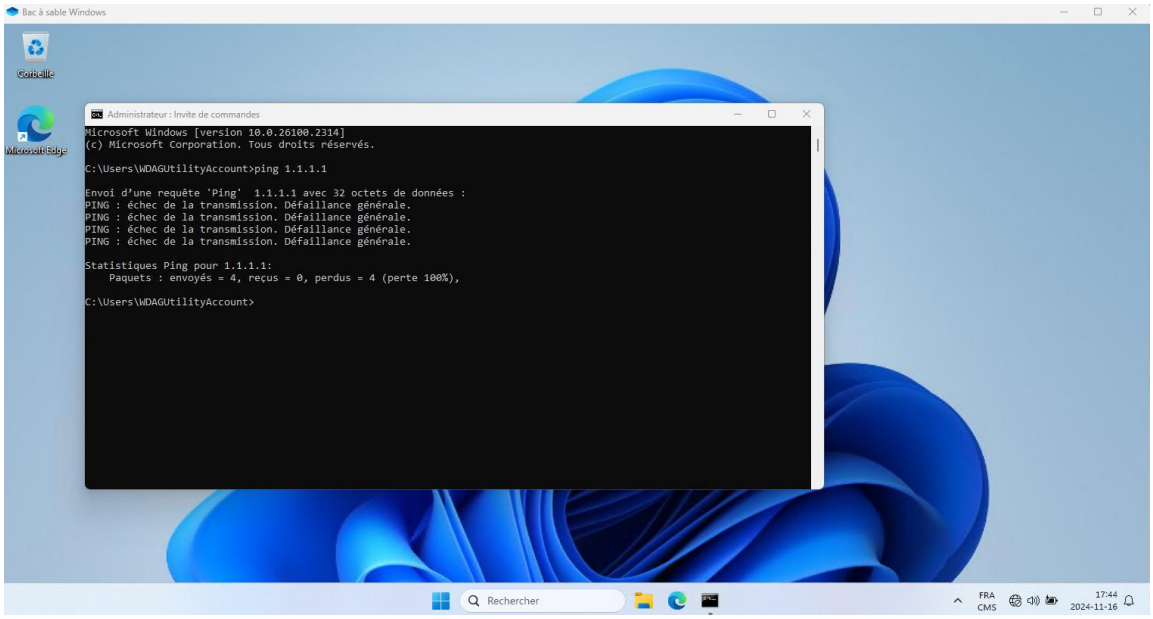
Configuration de la Windows Sandbox (2 points)

1. Créez un fichier de configuration Windows SandBox (.WSB) afin de couper la connexion réseau de la Sandbox. Quel est le contenu de ce fichier ?

Fichier Modifier Affichage

```
<configuration>
<networking>disable</networking>
</configuration>
```

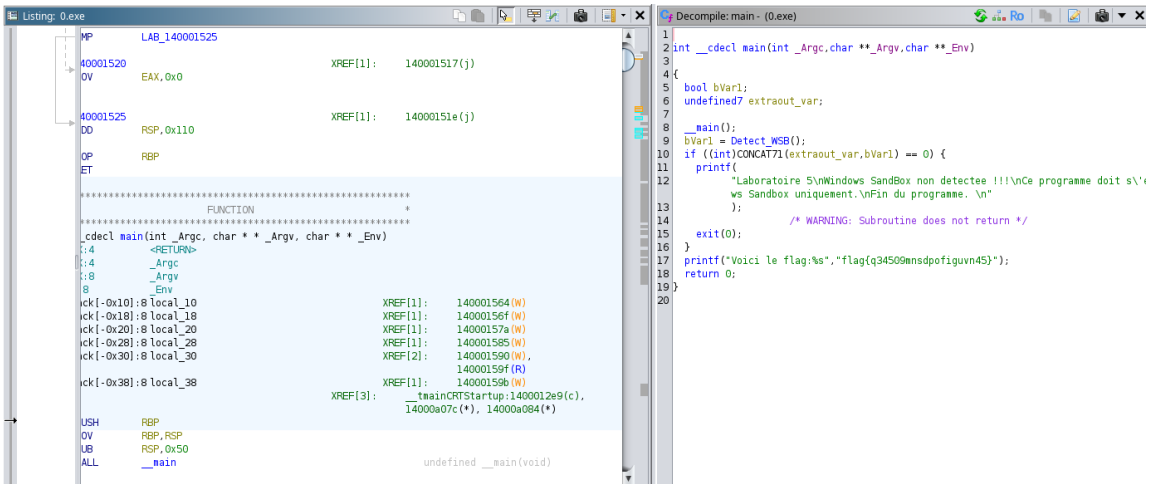
2. Montrer que la Windows SandBox est déconnectée en faisant une capture écran de la commande ping 1.1.1.1



Exercice 0.exe : analyse statique et dynamique

Le programme 0.exe affiche un flag dans le terminal de commande (cmd).

1. Sous kali linux, faites une analyse statique via Ghidra pour trouver le flag affiché. Copiez ci-dessous une capture écran du code de 0.exe :



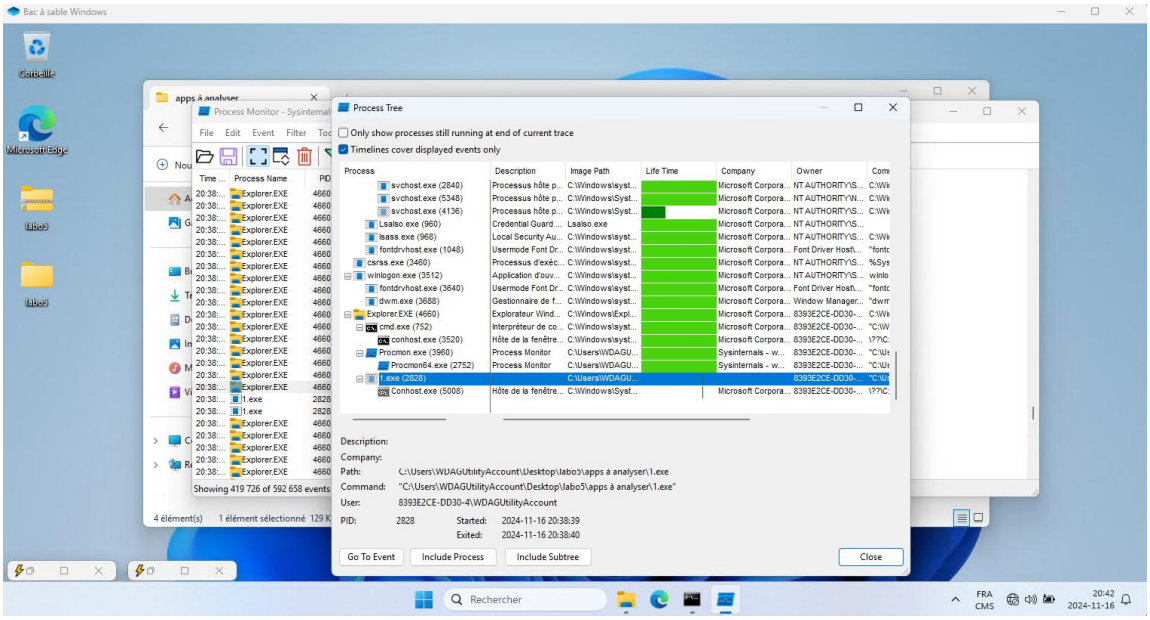
2. Sous la Windows Sandbox, exécutez le programme. Quel est le flag ?

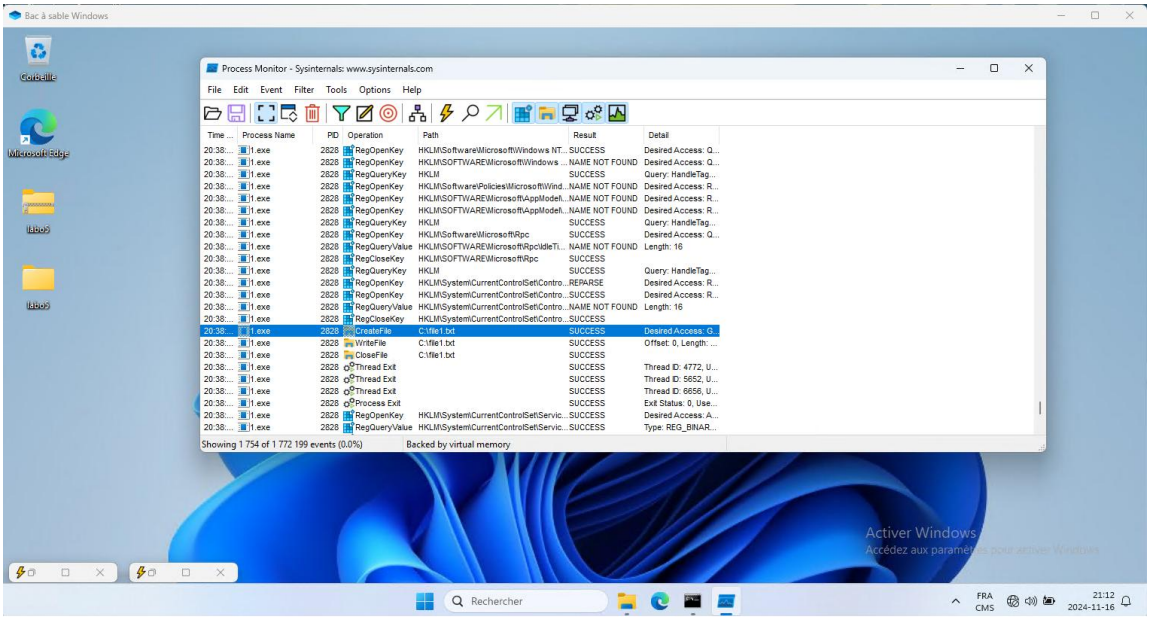
```
 Répertoire de C:\Users\WDAGUtilityAccount\Desktop\labo5

2024-11-16  17:46    <DIR>          .
2024-11-16  17:46    <DIR>          ..
2024-11-16  17:46    <DIR>          apps à analyser
2024-11-16  17:46    <DIR>          tools
               0 fichier(s)                0 octets
               4 Rép(s)  82 915 663 872 octets libres

C:\Users\WDAGUtilityAccount\Desktop\labo5>cd "apps à analyser"

C:\Users\WDAGUtilityAccount\Desktop\labo5\apps à analyser>dir
 Le volume dans le lecteur C n'a pas de nom.
 Le numéro de série du volume est 5AFF-822D

 Répertoire de C:\Users\WDAGUtilityAccount\Desktop\labo5\apps à analyser

2024-11-16  17:46    <DIR>          .
2024-11-16  17:46    <DIR>          ..
2023-11-19  17:05           246 777 0.exe
2023-11-19  17:06           132 950 1.exe
2023-11-19  17:05           133 699 2.exe
2023-11-19  17:06           132 795 3.exe
               4 fichier(s)          646 221 octets
               2 Rép(s)  82 915 565 568 octets libres

C:\Users\WDAGUtilityAccount\Desktop\labo5\apps à analyser>0.exe
Voici le flag:flag{q34509mnsdpofiguvn45}
C:\Users\WDAGUtilityAccount\Desktop\labo5\apps à analyser>
```

Exercice 1.exe : analyse dynamique – fichier

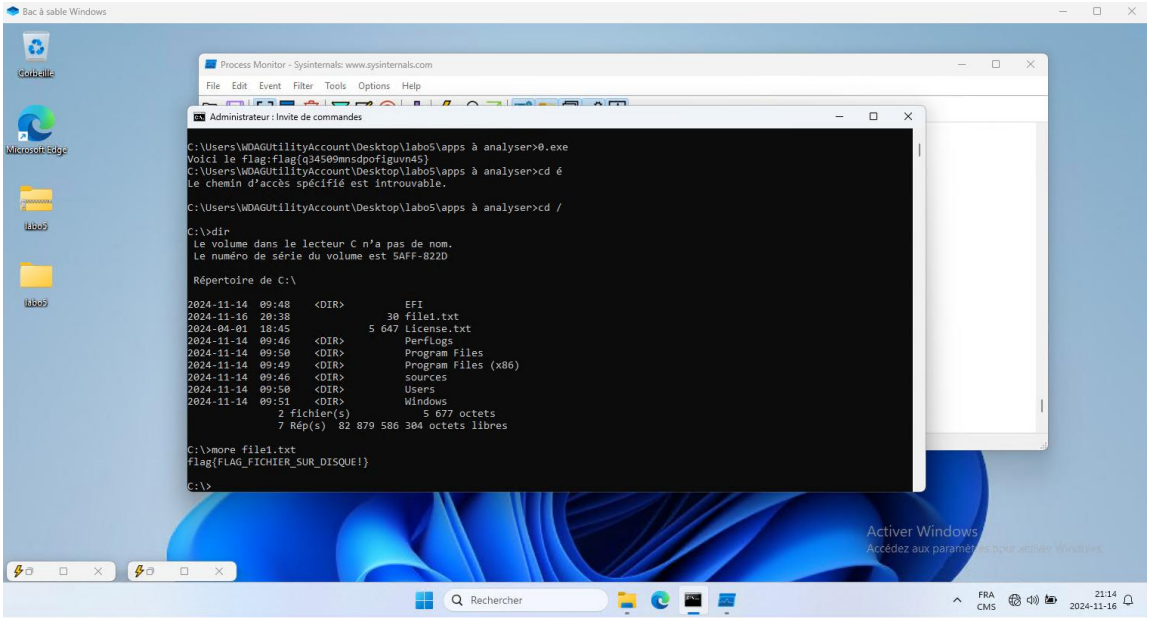
Le programme 1.exe crée un fichier. Sous la Windows Sandbox, utilisez le programme ProcMon pour trouver le flag.

1. Comment avez-vous trouvé le fichier avec Procmon ? (capture écran)





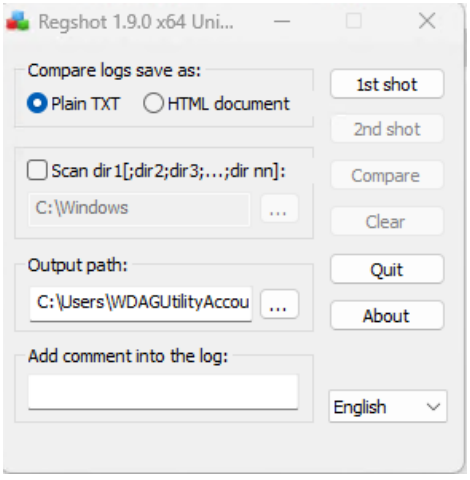
2. Quel est le flag ?

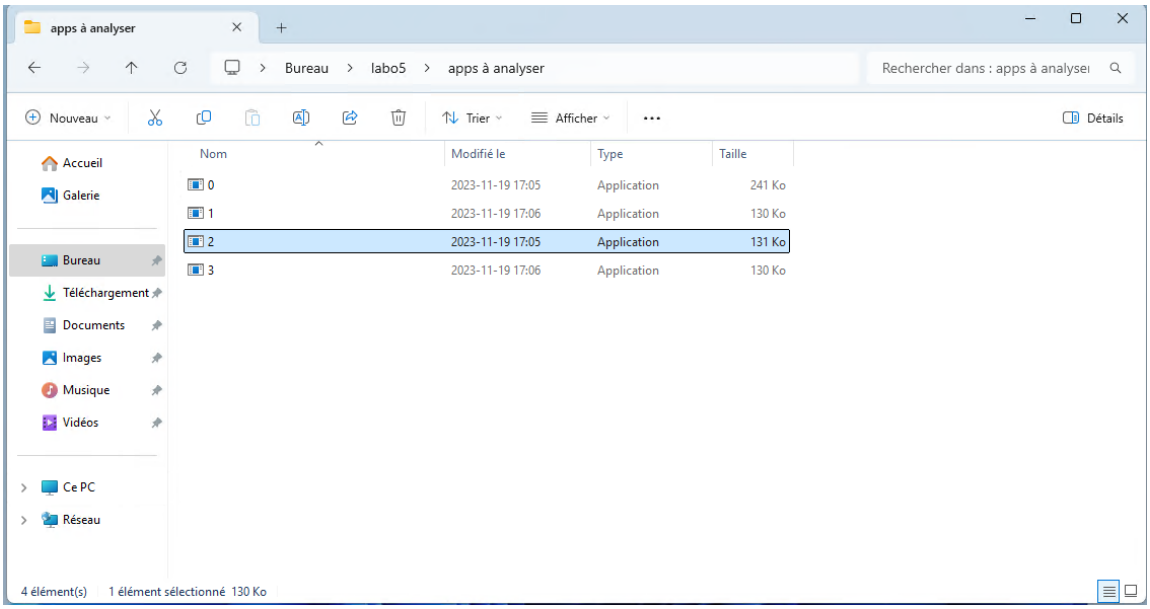


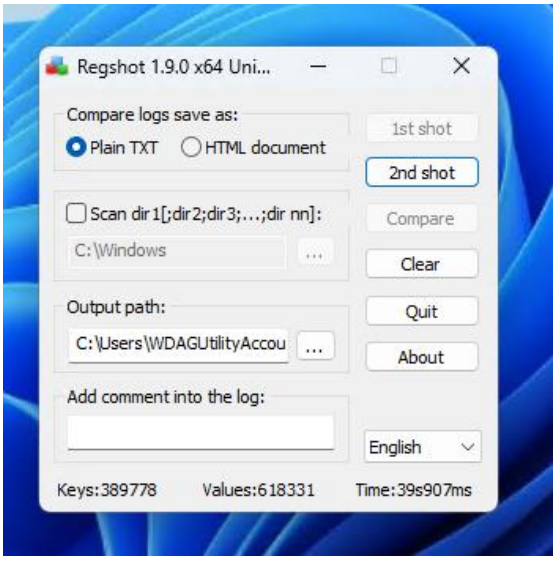
Exercice 2.exe : analyse dynamique – base de registre

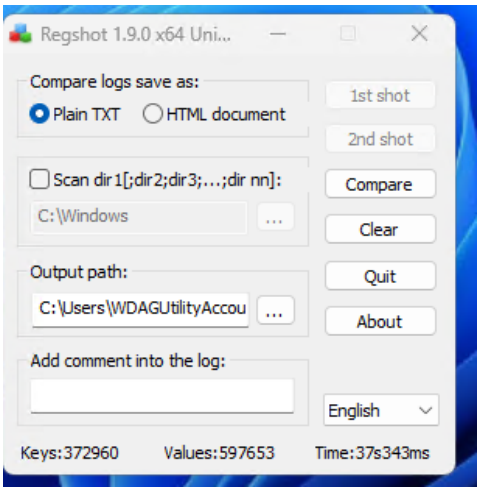
Le programme 2.exe crée une entrée dans la base de registre. Sous la Windows Sandbox, utilisez le programme RegShot pour trouver le flag.

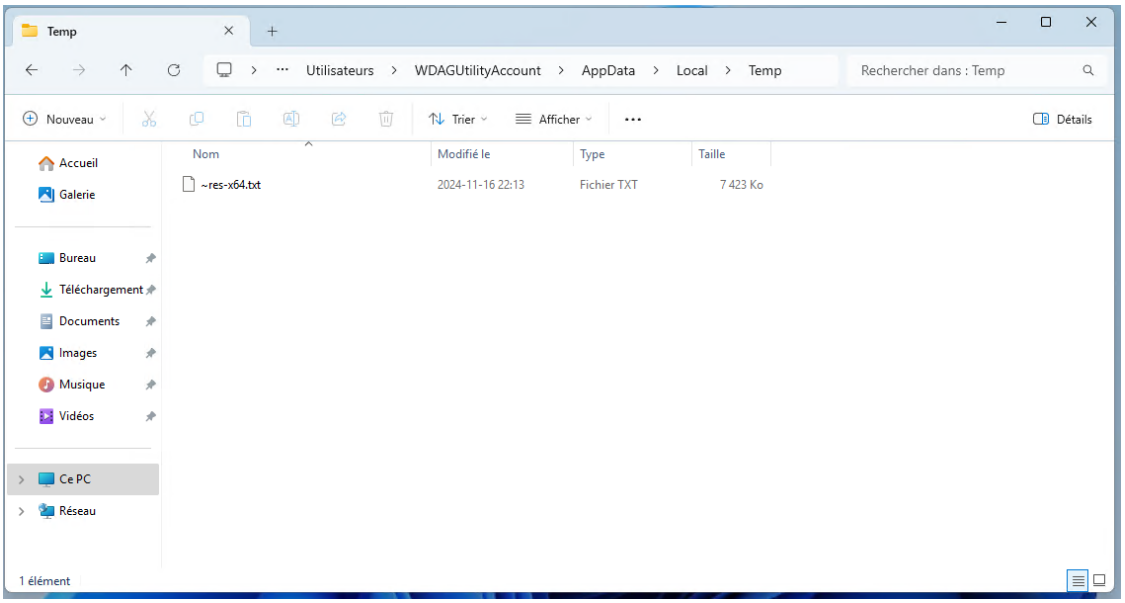
1. Comment avez-vous trouvé le flag avec RegShot ? (capture écran)




apps à analyser
Bureau
labo5
apps à analyser
Rechercher dans : apps à analyser
Nouveau
Trier
Afficher
Détails
Accueil
Galerie
Bureau
Téléchargement
Documents
Images
Musique
Vidéos
Ce PC
Réseau
Nom
Modifié le
Type
Taille
0 2023-11-19 17:05 Application 241 Ko
1 2023-11-19 17:06 Application 130 Ko
2 2023-11-19 17:05 Application 131 Ko
3 2023-11-19 17:06 Application 130 Ko
4 élément(s)
1 élément sélectionné 130 Ko


Regshot 1.9.0 x64 Uni...
Compare logs save as:
Plain TXT
HTML document
Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows
Output path:
C:\Users\WDAGUtilityAccou
Add comment into the log:
1st shot
2nd shot
Compare
Clear
Quit
About
English
Keys:389778
Values:618331
Time:39s907ms


Regshot 1.9.0 x64 Uni...
Compare logs save as:
Plain TXT
HTML document
Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows
Output path:
C:\Users\WDAGUtilityAccou
Add comment into the log:
1st shot
2nd shot
Compare
Clear
Quit
About
English
Keys:372960
Values:597653
Time:37s343ms



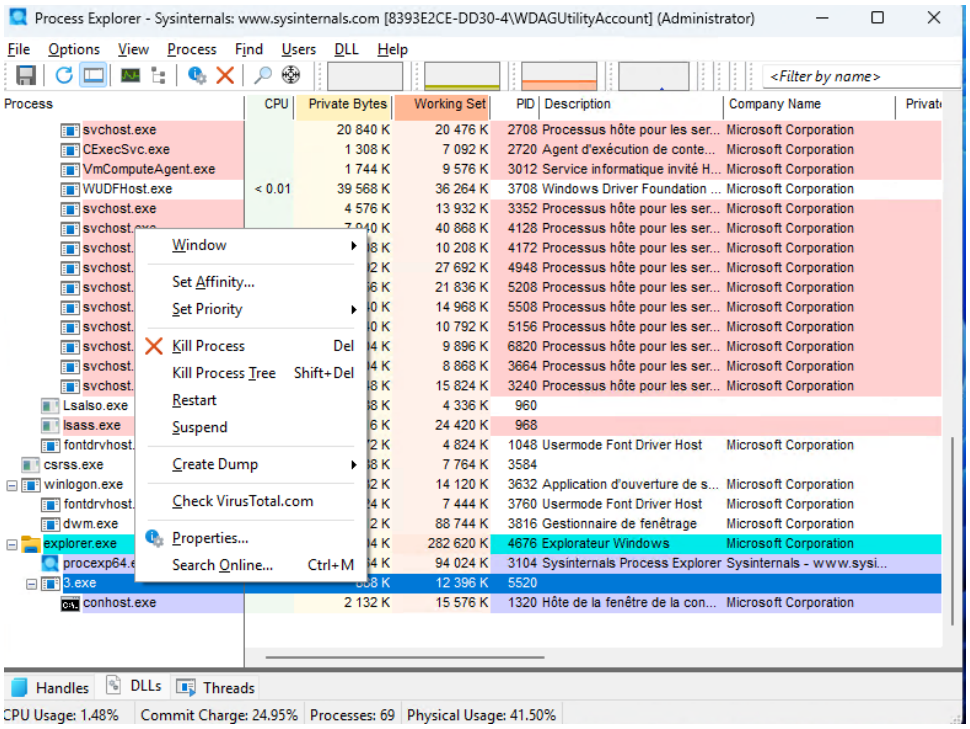
2. Quel est le flag ?

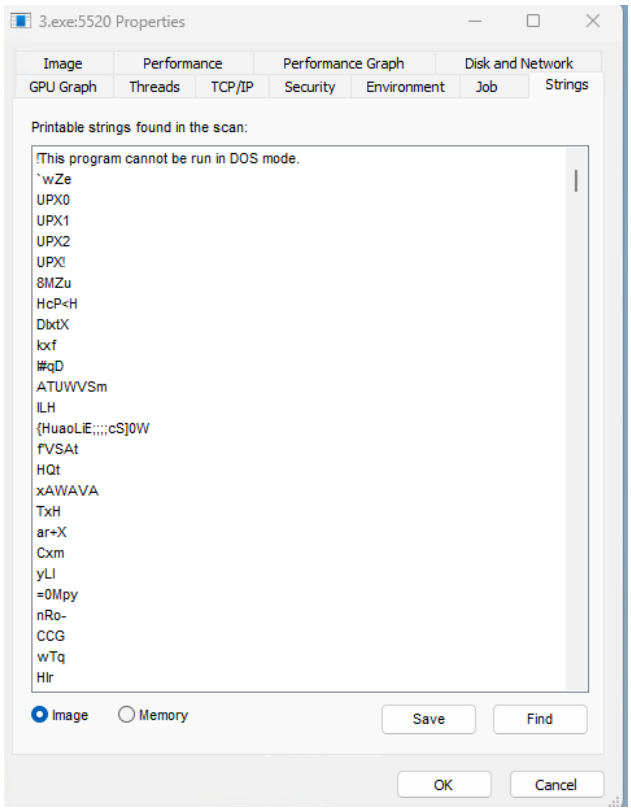
```
----------------------------------
Values added: 42
----------------------------------
HKLM\SOFTWARE\Microsoft\Security Center\cval: 0x00000001
HKLM\SOFTWARE\Microsoft\Security Center\Provider\Av\DataMigrated: 0x00000001
HKLM\SOFTWARE\Microsoft\Security Center\Provider\Fw\DataMigrated: 0x00000001
HKLM\SOFTWARE\Microsoft\Security Center\Svc\VistaSp1:  12 2F 73 0F 96 38 DB 01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\labo5: "flag{APP_IN_REGISTRY!}"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\WinREUninstallList\Timestamp: "2024-11-17T02:11:47Z"
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2047949552-857980807-821054962-504\\Device
\HarddiskVolume2\Users\WDAGUtilityAccount\Desktop\labo5\apps à analyser\2.exe:  37 D4 EF 21 96 38 DB 01 00 00 00 00 00 00
00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2047949552-857980807-821054962-504\\Device
\HarddiskVolume2\Users\WDAGUtilityAccount\Desktop\labo5\apps à analyser\2.exe:  37 D4 EF 21 96 38 DB 01 00 00 00 00 00 00
00 00 00 00 00 00 02 00 00 00
HKU\S-1-5-19\Software\Microsoft\Multimedia\msacm.imaadpcm\MaxRTEncodeSetting: 0x00000006
HKU\S-1-5-19\Software\Microsoft\Multimedia\msacm.imaadpcm\MaxRTDecodeSetting: 0x00000006
HKU\S-1-5-19\Software\Microsoft\Multimedia\msacm.msgsm610\MaxRTEncodeSetting: 0x00000004
HKU\S-1-5-19\Software\Microsoft\Multimedia\msacm.msgsm610\MaxRTDecodeSetting: 0x00000004
HKU\S-1-5-21-2047949552-857980807-821054962-504\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-
ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\JQNTHgvyvglNppbhag\Qrfxgbc\ynob5\nccf à nanylfre\2.rkr:  00 00 00 00 02 00 00
00 00 00 00 00 6D 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF
00 00 80 BF 00 00 80 BF FF FF FF FF E0 57 DC 21 96 38 DB 01 00 00 00 00
HKU\S-1-5-21-2047949552-857980807-821054962-504\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage
\KeyCreationTime:  E4 2C ED 24 96 38 DB 01
```

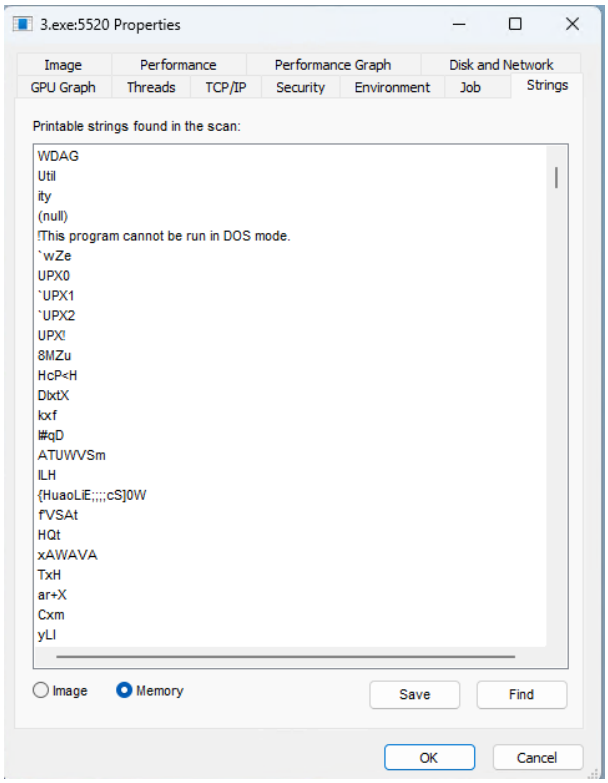

Exercice 3.exe : analyse dynamique – mémoire

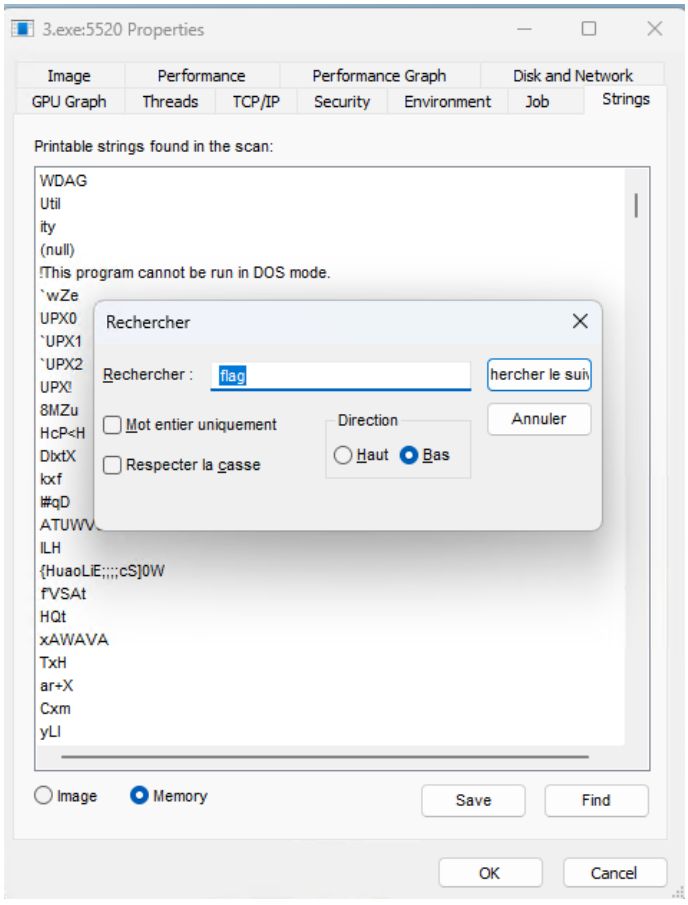
Le programme 3.exe copie un flag dans la mémoire RAM de la SandBox. Sous la Windows Sandbox, utilisez le programme Process Explorer pour trouver le flag dans la mémoire.

1. Comment avez-vous trouvé le flag dans la mémoire avec Process Explorer ? (capture écran)






3.exe:5520 Properties
Image
Performance
Performance Graph
Disk and Network
GPU Graph
Threads
TCP/IP
Security
Environment
Job
Strings
Printable strings found in the scan:
WDAG
Util
ity
(null)
!This program cannot be run in DOS mode.
`wZe
UPX0
`UPX1
`UPX2
UPX!
8MZu
HcP<H
DlxtX
kxf
l#qD
ATUWVSm
lLH
{HuaoLiE;;;;cS]0W
f'VSAt
HQt
xAWAVA
TxH
ar+X
Cxm
yLI
Image
Memory
Save
Find
OK
Cancel


3.exe:5520 Properties
Image
Performance
Performance Graph
Disk and Network
GPU Graph
Threads
TCP/IP
Security
Environment
Job
Strings
Printable strings found in the scan:
WDAG
Util
ity
(null)
!This program cannot be run in DOS mode.
`wZe
UPX0
`UPX1
`UPX2
UPX!
8MZu
HcP<H
DlxtX
kxf
l#qD
ATUWV
lLH
{HuaoLiE;;;;cS]0W
f'VSAt
HQt
xAWAVA
TxH
ar+X
Cxm
yLI
Rechercher
Rechercher :
flag
hercher le sui
Annuler
Mot entier uniquement
Respecter la casse
Direction
Haut
Bas
Image
Memory
Save
Find
OK
Cancel

2. Quel est le flag ?